May 28, 2015 Volume 8, Issue 10

Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
CAB	Thu, Jun 4 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
Registrar Refresher Training	Thu, Jun 11 2:30 to 3:30	Telecon	888-455-1864 Passcode: 3611044 NEW PASSCODE
User Group	Tue, Jun 16 9:00 to 12:00	GSA Central Office 1800F St. NW Conference Rm. 3046	888-455-1864 Passcode: 5887966
Derived Credential Working Group	Wed, Jun 17 10:00 to 11:30	GSA Central Office 1800F St. NW Conference Rm. 7115	866-556-0154, Passcode: 2132069
Non-PIV Working Group	Wed, Jun 17 12:30 to 2:00	GSA Central Office 1800F St. NW Conference Rm. 7115	866-556-0154, Passcode: 2132069
Registrar Classroom Training	Wed and Thu Jun 10-11 Jul 15-16 Aug 12-13	HP Chantilly, VA	Contact Jim Schoening for information or to Register

GSA

USAccess Program

Special Points of Note:

Now found on www.fedidcard.gov:

- **Service Order Requests and Test Card Orders**
- **Role Holder Web Based Training Registration**
- **Deployment Activities and USAccess Center Status Alert**
- **Contact Steve Sill (Stephen.sill@gsa.gov) to be added to User Group (UG) distribution list.**
- **Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up**

USAccess Non-PIV Working Group Established

On May 7, 2015 the CAB voted to establish a USAccess Non-PIV Working Group (NPWG). The purpose of the NPWG is to identify and discuss the use cases and various types of Non-PIV credentials, such as PIV-I and Temporary Cards, and provide a recommendation to the CAB as to what the USAccess program needs to offer, if needed.

The NPWG will meet for the first time on Wednesday, June 17 from 12:30 p.m. - 2:00 p.m at GSA, 1800 F Street NW, Washington, DC, in Room 7115.

Working Group membership will be established based on those in attendance at the meeting and those that express interest if they are unable to attend the first meeting.

Inside this issue:

Fixed Infrastructure Windows 7 Workstation Replacement Update

The schedule for fixed workstation replacement is posted on the Agency Lead Portal (ALP). This schedule includes the planned timeframes for fixed site Prep Calls, Windows 7 equipment shipments and Install Calls.

Prep Calls Completed for All Waves

Prep calls were completed for all Waves. All but one Agency completed their prep calls and the MSO is in discussions with the impacted site. We appreciate your efforts to have your sites attend these calls as they are a critical step to ensuring sites understand the process and their responsibilities.

Windows 7 Equipment Shipping

Equipment has shipped for Waves 1-9. Wave 10 should complete shipping by end of this week.

Emails were sent to site POCs with shipment tracking information and instructions for preparing for the install call. Please look for the shipment email and be sure to follow the steps to prepare for and schedule the install call within 2 weeks of equipment arrival on site.

Install Calls/Site Recertifications

As of Friday, May 22, we certified/held install calls for 150 sites and are more than halfway to our goal of upgrading all fixed centers to Windows 7.

As a reminder, please prepare for your Install Calls. When a site completes the following steps before the call, we can complete an install in about an hour. When they are not completed, **they can take up to 3 hours.**

Please complete the following before your install call:

- Registrars/Activators know UPN/Password (refer to USAccess Windows 7 Workstation Replacement Guide)
- Set up Windows 7 machines 1 hour prior to install call (refer to USAccess Win 7 Quick Install Guide)
- Line up Applicant to activate or update card during install call (needed to recertify site)
- Have Site POC, Local IT and Registrars/Activators on call

Fixed Infrastructure Windows 7 Workstation Replacement Update Continued

Weekly Reports—Please reach out to MSO if you have not received them

Reports are sent to the MSO on a weekly basis (on Mondays) that show Agency Leads the schedule for their fixed sites, as well as their progress in meeting all of their milestones. If you have not received a report, please reach out to the MSO.

New Interagency Agreement Training Available

New training is available to assist Finance personnel in correctly filling out Interagency Agreements and addendums. The training is posted on the Agency Lead Portal. The IA training can be found here.

Finance Reminder

As a reminder to all of our customer agencies, please be sure to maintain sufficient funding for your HSPD-12 services. The IA addendum form used to obligate additional funding and instructions for completing it can be found on the FedIDcard.gov website under the Customer Agencies tab in the Onboarding Process section. Please feel free to contact Spiro Papagjika (spiro.papagjika@gsa.gov) or Meredith Rose (Meredith.rose@gsa.gov) with any funding-related questions.

Service Enhancements

Planned Changes

- **Maintenance is scheduled for Saturday, May 30 from 5:30 a.m. to 8:00 p.m. Please plan for the USAccess Service and role holder portals to be unavailable for most of the day.**

Security Tip

USAccess Role Holder Rules of Behavior Review

Access to USAccess requires that each Role Holder review and sign the USAccess Rules of Behavior. At a minimum the USAccess Rules of Behavior includes:

1. Safeguarding user ID's, passwords and personal identification numbers (PINs).

   a. Role Holders are prohibited from disclosing this information to anyone, regardless of their position in or outside of your agency

   b. However, Role Holders may be required to reveal this information to the Information System Security Officer (ISSO) or IT staff if so directed by with a written request form their agency management

2. Accountability for all entries and changes made to USAccess using their passwords and PINs. This implies that Role Holders will not:

   a. Permit others to use their user ID, personal passwords or PINs

   b. Use another Role Holder's user ID, personal password or PIN.

3. Immediately report any misuse or compromise of user ID's, passwords or PINs to the ISSO or local Help Desk.

4. Ensure that a lost, stolen PIV card is immediately reported to their ISSO or local Help Desk.

5. Understand and agrees to USAccess and their agency regulations and security policies designed to ensure the confidentiality of all sensitive information.

6. Understand and acknowledge that any information concerning agency credential holders is confidential and protected from unauthorized disclosure by law.

7. Understand and acknowledge that unauthorized access or modification to USAccess records is not permitted

8. Understand and acknowledge that improper disclosure of USAccess credential related information to anyone not authorized to receive it may result in substantial fines and penalties under the Privacy Act of 1974.